

## **Remarks**

### **1. Introduction**

Claims 5-28 are pending. Claims 5 and 17 are independent claims.

### **2. Rejection based on 35 U.S.C. §101**

Claim 4 was rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicants cancel claim 4, rendering the rejection moot.

### **3. Rejection based on 35 U.S.C. §102**

Claims 1-4 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Number 6,735,768 (“Tanaka”).

Claims 5 and 17 recite limitations that relate to limiting execution of functions on an information processing device. Specifically, it is determined whether or not to execute a function in a stored content based on (1) the type of functions to be executed and (2) based on where the content is stored. As discussed in the present application, a user may not wish to have certain functions executed on an information processing device (such as a mobile phone). For example, a user may not wish for certain functions that attempt to access private information about the mobile phone, such as the mobile phone telephone number, to be executed. In order to prevent content stored on the mobile phone from performing the undesired functions, the information processing device determines “whether to prohibit execution of a function in at least a part of the content based on whether the content is stored in the first storage area and based on the function.” See claims 5 and 17. Specifically, depending on whether the content is stored (such as in the first storage area that indicates the content is for limited use) and depending on the type of function to be executed, the information processing device may determine whether to execute the function. For example, if a function relates to “obtaining information about the information processing device” (see claims 10 and 22), such as “obtaining identification information for the information processing device (see claims 11 and 23), the information processing device may disallow execution of the function if the content is stored in the cache memory. The listing of prohibited functions may be stored in the

mobile phone prior to storing the content, and may be a part of the operating system. See claims 12, 14, 24, and 26. In this way, the information processing device may control which functions may be executed even before the program is installed on the information processing device.

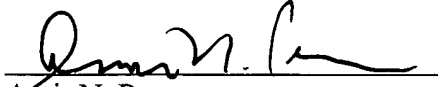
In contrast, the Tanaka reference does not teach or even suggest determining whether to execute a function in a program based on the type of function to be executed or based on the place where the program is stored. As an initial matter, the Tanaka reference is directed to an entirely different problem – whether to allow a device access to various functions in a software program. Specifically, the Tanaka reference is directed to preventing an unauthorized user from using a software program. Thus, Tanaka is directed to the opposite problem – the software program controlling whether to allow the user to access certain functions in the software program – and not the mobile phone (or other device) controlling whether to allow certain functions in the software program to be executed.

Moreover, the sections in the Tanaka reference cited in the Office Action do not relate to the electronic device, upon which the software program is resident, dictating whether to limit execution of the functions. Instead, the Tanaka reference teaches inputting a key code K in order to access various functions of a software program. Col. 2, lines 23-32. Further, the Tanaka reference teaches that in order to write the software program to the hard drive HD, the user must be authorized. Specifically, the coefficient checker 12 confirms whether the user is authorized based on two coefficient codes and a timestamp. See col. 6, lines 10-28. The authorization is not based on where the software program is installed or what functions are in the software program. Similarly, the Tanaka reference teaches that in order to execute the program, the user must be authorized. Specifically, the registration information checker 12 confirms whether the user is authorized based on two coefficient codes and a timestamp. See col. 6, lines 30-49. Again, the authorization is not based on where the software program is installed or what functions are in the software program. Thus, the Tanaka reference fails to teach, or even suggest, the limitations as claimed. Therefore, Applicants contend that the claims as currently presented are patentable over the cited art.

**4. Conclusion**

If any questions arise or issues remain, the Examiner is invited to contact the undersigned at the number listed below in order to expedite disposition of this application.

Respectfully submitted,

  
A handwritten signature in black ink, appearing to read "Amir N. Penn", is written over a horizontal line.

Amir N. Penn  
Registration No. 40,767  
Attorney for Applicant

BRINKS HOFER GILSON & LIONE  
P.O. BOX 10395  
CHICAGO, ILLINOIS 60610  
(312) 321-4200